IJARES/July 2015/Volume-3/Issue-7/1966-1970 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

A LIABLE APPROACH TOWARDS DEFENDING OF CLOUD DATA MAINTAINING ANONYMOUS VALIDATION

K.Uday Kiran[1], N.Vijaya Sunder Sagar[2], B.Goutham[3], Gongidi Shiva Krishna[4]

[1,3]**Assistant Professor, Dept of CSE, Ashoka Institute of Engineering and Technology, Hyderabad, T.S, India**

[2]**Associate Professor & HOD, Dept of CSE, Ashoka Institute of Engineering and Technology, Hyderabad, T.S, India**

[4]**M.Tech, Dept of CSE, Ashoka Institute of Engineering and Technology, Hyderabad, T.S, India**

ABSTRACT:

Access control within clouds is gaining concentration since it is essential that only approved users have access to applicable service. Attribute-based access control is more comprehensive in possibility where users are specified attributes, along with the data attaching access policy. An area where access control is extensively being employed is health care. Clouds are being employed to accumulate susceptible information concerning patients to facilitate access to medical professionals along with policy makers. We put forward privacy preserving authenticated access control system and according to system a user can generate a file and accumulate it securely in the cloud. This system consists of utilizing of two protocols such as attribute-based encryption as well as attribute-based signature (ABS). ABS is combined with ABE to attain authenticated access control devoid of disclosing the identity of the user towards the cloud. In the projected system, cloud verifies the dependability of series devoid of knowing the user's identity earlier than storing data. The projected scheme is challenging to repeat attacks, where user restores fresh data with stale data from a preceding write, although it no longer has applicable claim policy. Most of the schemes do not hold user revocation, which our system carries out. System has the additional feature of access control in which merely applicable users

are capable to decrypt the accumulated information.

Keywords: Access control, Clouds, Attribute-based signature, Privacy preserving.

1. INTRODUCTION:

Security as well as protection of privacy within clouds is being explored by numerous researchers. Clouds can make available quite a lot of types of services like applications infrastructures as well as platforms to assist developers write Applications [1]. Liability of clouds is an extremely tricky task and involves technical issues as well as law enforcement. Neither clouds nor users have to deny any operations executed. It is significant to have log of transactions performed; however, it is a significant concern to make a decision regarding information to maintain in the log. Access control is moreover gaining significance in online social networking where users accumulate their personal information, videos and allocate them with particular groups of users they belong to [2]. A vast amount of information is being accumulated inside the cloud. There are generally three types of access control such as user-based access control, role-based access control, as well as attribute-based access control. We use attribute-based access control scheme to accomplish authenticity as well as privacy. Attribute-based access control is more comprehensive in possibility where users are specified attributes, along with the data attaching access policy. We put forward a new scheme of decentralized access control in support of safe data storage within clouds that sustain anonymous validation. In the projected system, cloud verifies the dependability of series devoid of knowing the user's identity earlier than storing data. Our system is tough and decentralized, for the most part of the others is centralized and maintains privacy preserving verification, which is not supported by others. The projected scheme is challenging to repeat attacks, where user restores fresh data with stale data from a preceding write, although it no longer has applicable claim policy. This is a significant property since a user, revoked of its attributes, may no longer be competent to write to the cloud [3]. Our plan moreover allows writing numerous times which was not legalized in previous work.

2. METHODOLOGY:

Resourceful search on encrypted data is in addition an essential concern in clouds. The

clouds must not know the query but have to be able to return the records that convince the query and this is achieved by searchable encryption. Authentication of users by means of public key cryptographic methods was studied. Numerous homomorphic encryption methods were recommended to guarantee that cloud is not proficient to read the data while executing computations on them. By means of homomorphic encryption, the clouds obtain ciphertext of data and carry out computations on the ciphertext and return the encoded assessment of result. An area where access control is extensively being employed is health care. Clouds are being employed to accumulate susceptible information concerning patients to facilitate access to medical professionals along with policy makers [4]. It is significant to manage the access of data with the intention that approved users access the information. By means of ABE, records are encrypted below several access policies and accumulated within the cloud. It is extremely significant that merely the approved users are provided access towards that information. A novel protocol recognized as attribute-based signature (ABS) has been functional. In ABS, users contain a claim predicate connected with a message [5]. We put forward a new scheme of decentralized access control in support of safe data storage within clouds that sustain anonymous validation. Our system is tough and decentralized, for the most part of the others are centralized. Our system moreover maintains privacy preserving verification, which is not supported by others. Most of the schemes do not hold user revocation, which our system carries out. Our system in addition has the additional feature of access control in which merely applicable users are capable to decrypt the accumulated information. The system put off replay attacks as well as supports creation, alteration, and reading data accumulated in the cloud. Authentication as well as access control system is decentralized as well as robust, unlike other access control systems designed in support of clouds which are centralized.

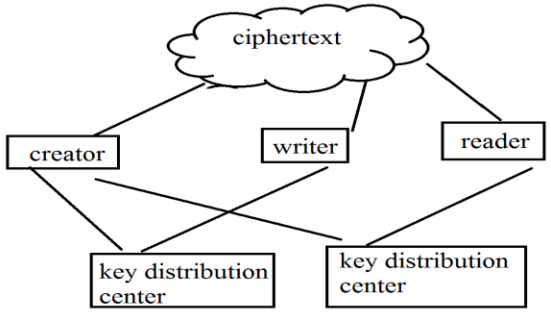

Fig1: An overview of secure cloud storage representation

3. AN OVERVIEW OF AUTHENTICATED ACCESS CONTROL SYSTEM:

Access control within clouds is gaining concentration since it is essential that only approved users have access to applicable service. We put forward privacy preserving authenticated access control system and according to system a user can generate a file and accumulate it securely in the cloud. This system consists of utilizing of two protocols such as ABE as well as attribute-based signature (ABS). The majority of the schemes do not hold user revocation, which our system carries out and has the additional feature of access control in which merely applicable users are capable to decrypt the accumulated information [6][7]. ABS is combined with ABE to attain authenticated access control devoid of disclosing the identity of the user towards the cloud. In ABE, a user contains a set of attributes additionally to its unique ID. Fig1 shows the projected model of secure cloud storage in which there are three users such as a creator, a reader, as well as writer. Creator C receives a token from trustee, who is supposed to be honest and who manages social insurance numbers. On presenting her id, trustee provides her a token. A creator on presenting the token to one or additional key distribution centre receives keys for encryption/decryption as well as signing. The access policy makes a decision of the person who wants to access the data accumulated in the cloud. The creator makes a decision on a claim policy, to establish her authenticity and signs message under this claim [8]. The cipher text by means of signature is sent towards the cloud which verifies the signature and accumulates the cipher text. If the user contains attributes corresponding with access policy, it decrypts and retrieve original message. By designating verification procedure towards the cloud, it alleviates the individual users from time intense verifications.

4. CONCLUSION:

Access control is moreover gaining significance in online social networking where users accumulate their personal information, videos and allocate them with particular groups of users they belong to. There are generally three types of access control such as user-based access control, role-based access control, as well as attribute-based access control. We put forward a new scheme of decentralized access control in support of safe data storage

within clouds that sustain anonymous validation. In the projected system, cloud verifies the dependability of series devoid of knowing the user's identity earlier than storing data. The projected scheme is challenging to repeat attacks, where user restores fresh data with stale data from a preceding write, although it no longer has applicable claim policy. Our system is tough and decentralized, for the most part of the others are centralized. Our system moreover maintains privacy preserving verification, which is not supported by others. Most of the schemes do not hold user revocation, which our system carries out. Our system in addition has the additional feature of access control in which merely applicable users are capable to decrypt the accumulated information.

REFERENCES

[1] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.

[2] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.

[3] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.

[4] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[5] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[6] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.

[7] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.